UNITED STATES
NAVAL WAR COLLEGE
Newport, RI

Operational Protection of Information Technology Assets

A Commander's Guide to Risk Reduction

by

Janice M. Hamby
Commander, United States Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

May 19, 1997

(Graduation November 1997)

Paper direct by Captain G. Jackson
Chairman, Joint Military Operations Department

W.F. Jurecka, CDR, USN — Faculty Advisor — 16 MAY 97 — Date

Security Classification This Page UNCLASSIFIED

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	
6. Office Symbol: C	**7. Address:** NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): Operational Protection of Information Technology Assets: A Commander's Guide to Risk Reduction (U)	
9. Personal Authors: CDR Janice M. Hamby, USN	
10.Type of Report: FINAL	**11. Date of Report:** 19 May 1997 (grad 11/97)
12.Page Count: 29	
13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.	
14. Ten key words that relate to your paper: INFORMATION, WARFARE, TECHNOLOGY, OPERATIONAL, PROTECTION, RISK, MANAGEMENT, IW, IT, C4I	

15.Abstract: **Information technology (IT) is an essential part of any military action.** The U.S. military increasingly relies on the force multiplier effect yielded by technological superiority and plans to conduct information warfare (IW) in future conflicts to minimize exposure and risk to forces. Despite the clear advantages that IT and IW can create for the combatant commander, their use is not risk free. Heavy dependence on IT yields a target rich environment for any adversary wishing to conduct his own IW campaign. Current developments in doctrine for IW do not adequately focus on thepotential ramifications of IW and fail to highlight the criticality of the function of defensive IW (IW-D) and the operational protection of our extended IT infrastructure. Thoughtful, methodical approaches to minimize risk are needed. This paper provides context for and proposes one such approach.

16.Distribution / Availability of Abstract:	**Unclassified**	**Same As Rpt**	**DTIC Users**
	X		

17.Abstract Security Classification: UNCLASSIFIED	
18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT	
19.Telephone: 841-6461	**20.Office Symbol:** C

Security Classification of This Page Unclassified

ABSTRACT

Information technology (IT) is an essential part of any military action. It is used to accomplish all operational functions and through all stages of the employment of forces in peacetime and in war. It has a positive effect on the use of space and time. The U.S. military increasingly relies upon the force multiplier effect yielded by technological superiority and plans to conduct information warfare (IW) in future conflicts to minimize exposure and risk to forces. Despite the clear advantages that IT and IW can create for the combatant commander, their use is not risk free. Heavy dependence on IT yields a target rich environment for any adversary wishing to conduct his own IW campaign. Current developments in doctrine for IW do not adequately focus on the potential ramifications of IW and fail to highlight the criticality of the function of defensive IW (IW-D) and the operational protection of our extended IT infrastructure.

The challenges presented by U.S. investment in and reliance upon IT and the intent to use offensive IW (IW-O) in future conflicts require thoughtful, methodical approaches to minimizing the risk entailed. This paper provides the combatant commander, and subordinate commanders, with a background for appreciating our IW/IT vulnerabilities. It begins by considering the elements of IW and the vulnerable elements in our IT infrastructure. A general discussion of the concept of operational protection and the IT and IW assets requiring protection in theater and at the strategic level follows. General threats to these systems are described. The paper concludes by proposing the use of Operational Risk Management (ORM) for developing and implementing an effective strategy of operational protection for IW and IT assets. It suggests an approach to tie these concepts together into a rational plan for minimizing risk and maximizing the commander's probability that he will indeed win the information war.

TABLE OF CONTENTS

Introduction

> **Information Warfare has emerged as a key joint warfighting mission area. The explosive proliferation of information-based technology significantly impacts warfighting across all phases, the range of military operations, and all levels of war.**[i]
>
> ***– General John M. Shalikashvili***

Information technology (IT) is an essential part of any military action. It is used to accomplish all operational functions and through all stages of the employment of forces in peacetime and in war. It has a positive effect on the use of space and time. The U.S. military increasingly relies upon the force multiplier effect yielded by technological superiority and plans to conduct information warfare (IW) in future conflicts to minimize exposure and risk to forces. Despite the clear advantages that IT and IW can create for the combatant commander, their use is not risk free. Heavy dependence on IT yields a target rich environment for any adversary wishing to conduct his own IW campaign. Current developments in doctrine for IW do not adequately focus on the potential ramifications of IW and fail to highlight the criticality of the function of defensive IW (IW-D) and the operational protection of our extended IT infrastructure.

The challenges presented by the investment in and reliance upon IT and the intent to use offensive IW (IW-O) in future conflicts require thoughtful, methodical approaches to minimizing the risk entailed. This paper provides the combatant commander, and subordinate commanders, with a background for appreciating such IW/IT vulnerabilities. It begins by considering the elements of IW and the vulnerable elements in the IT infrastructure. A general discussion of the concept of operational protection and the IT and IW assets requiring

protection in theater and at the strategic level follows. Threats to these systems are described. The paper concludes by proposing the use of Operational Risk Management (ORM) for developing and implementing an effective strategy of operational protection for IW and IT assets. Its approach ties these concepts together into a rational plan for minimizing risk and maximizing the commander's probability that he will indeed win the information war.

Background

Long ago the United States' use of IT passed the threshold that defines its continued, reliable function as a vital interest. Commercial systems are essential to socio-economic well being and to defense. Transactions across financial networks, transmissions across voice and data circuits, automated control of air and rail transport systems...these are just a few examples of publicly controlled IT that are both essential to commerce and integrated with defense systems to support military communications, logistics and administration. The leverage gained from information systems is countered by the vulnerabilities created by that dependence. National security, in the broadest sense of the term, relies on the integrity of our information and information processes.

The 1996 National Security Strategy recognizes the key roles of IT and the National Information Infrastructure (NII), the "electronic superhighway." It cites "threat of intrusions to our military and commercial information systems" as significant risks.[2] The National Military Strategy notes the "remarkable leverage attainable from modern reconnaissance, intelligence collection and analysis, and high-speed data processing and transmission" and highlights the combatant

commander's need for fused information systems[3] Fighting and winning the information war is a clear objective for U.S. forces.

All four services are developing IW doctrine based on Operation Desert Storm's IW success. The focus is on IW-O with an additional charge to prevent the enemy's successful conduct of IW against friendly forces. This focus is backwards. IW-D is more important to our military operations than IW-O. The old saw 'the best defense is a good offense' holds true only if the offense is focused on combating threats to our own IT investment. Stephen Kent, chief scientist for security technology, Bolt Beranek and Newman, Inc., captures the essence of the problem, "In information warfare, offensive forces have an enormous advantage over defensive forces."[4] Single micro-computers with modems and readily available software can attack entire networks. Accepted defense-to-offense ratios simply do not apply. The extended infrastructure is like an overextended front line – extremely vulnerable to attack and needing reinforcement. The operational commander must deliberately act to minimize the risk that essential information systems will fail or will succumb to attack at a pivotal moment. This process must start long before any crisis erupts to call the military into action. It is one for consideration by any erstwhile operational commander before the mantle of theater command is cast his direction.

IW -- What is It?

Because IW is relatively young, there is no single accepted definition. Some argue that it comprises any use of information systems to gain an advantage in war. This includes the administrative use of computers for

processing logistics or reports and is too broad. Others limit IW to the several areas that are sufficiently developed to have accepted doctrine such as command and control warfare (C2W) and psychological operations (PSYOPS.) Confusing the issue further is the valid point that IW is not limited to the military sphere or to conduct by military forces. Indeed, IW "spans the spectrum of political, economic, physical and military activities..[5] In the extended context, the term "information operations" is now in vogue.

The military definition of IW describes the "actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks."[6] It does not consider as IW assets all of the systems that IW-D is expected to defend (*e.g.* inventory tracking systems or personnel administration systems.)[7] The commander's plan for conducting IW-D must consider all IT assets upon which he relies to gain information superiority. Strategically, the IW battlespace extends outside of the theater. Comprehensive IW-D relies upon actions taken by other agencies and by commercial industry.

The IW Battlespace

The total IW battlespace literally spans the globe. Agents may be nations, political groups, coalitions, religious groups or military groups. Interactions range from cooperation through competition to conflict and ultimately war.[8] From the operational commander's perspective, the IW battlespace is focused within the theater of operations. It comprises his potential IW-O targets and the command,

control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) systems and general-purpose information systems used by his staff and assigned forces. The full suite of C4ISR and information systems includes those used to prosecute IW-O and those used for staff support. Both subsets are potential targets for the enemy. IT assets outside of the theater of operations connect the operational commander to additional support elements and to senior commands. He depends on their reliability and must understand their vulnerability.

Intra-theater

IT assets inside the theater are either stand-alone systems or networked systems. Stand-alones do require protection from enemy IW-O, but the problem is much simpler than for networked systems. Physical protection, emanations security, procedures standardization and user education are typically sufficient safeguards for stand-alone devices. Enforcement of standards and procedures is key to protecting the information processed on them.[9] Devices relying upon active emissions to perform their missions, such as air defense radar, require additional defense elements which may be an integral part of the systems.

Networked systems expand the problem of system security. They typically have a larger footprint (*i.e.* they are spread out, possibly between facilities, trailers or buildings,) more personnel involved in their operation, more access points (and signals emanation points,) and process higher volumes of data. Additionally, staffs tend to depend more heavily upon networked systems due to the inherent advantages of data and process sharing and communications

facilitation. A networked IT system solely used in a single controlled locale is commonly referred to as a local area network (LAN). LAN protection is an expanded problem, but it is essentially the same as that for stand-alone systems.

Unfortunately (for those tasked with providing systems security), networked systems are not usually contained within a controlled locale. They extend throughout the theater into wide area networks (WANs) covering many kilometers over various media. This extended connectivity allows the commander to gain a better view of theater operations, share information with assigned forces, and allows various sensor and weapons systems to share data. This connectivity is a linchpin in the process of securing information superiority. It is also a key target for C2W, one of the pillars of IW-O.

Extra-theater

The operational commander's WANs and some LANs will be connected to systems outside of the theater of operations. He will also control some individual systems that are local connections to someone else's network. These connections tie him into the Defense Information Infrastructure (DII). The DII is operated as "a utility to support war fighting, intelligence and business functions"[10] and is a subset of the National Information Infrastructure (NII).[11] Classified sections of the DII are covered by traditional protection afforded by encryption and access control. This may protect data held and processed on the DII, but it does not guarantee the DII's security. The DII depends on reliable function of the U.S. power grid and public switched telecommunications. Over 95% of the DII voice and data traffic travels on the public telephone system.[12]

Unclassified defense systems (including most logistics systems) are connected to commercial systems that are connected to other systems. The intimate existence of the DII with commercial systems increases its vulnerability.[13] A successful IW attack on unprotected civilian infrastructure assets could render defense systems temporarily disabled or decrease their reliability to the point where they are effectively disabled.[14]

Does IT Need Operational Protection or Strategic Protection?

> **Government and commercial computer systems are so poorly protected today that they can essentially be considered defenseless – an electronic Pearl Harbor waiting to happen.[15]**
>
> ***– Winn Schwartau***

"Protecting one's own and friendly forces from a wide range of threats is one of the commander's most important responsibilities."[16] It is intended to ensure that when the decisive time and place coincide, friendly forces and assets are ready for employment. It entails deliberate efforts to counter the enemy's maneuver and firepower by making forces and assets difficult to locate, strike and destroy. It includes protecting forces and assets against natural disasters.[17] For assets that are complex systems, it must also protect against human error and accident. The operational commander's task is complicated by the fact that the function of his IT assets involves lines of communication (LOCs) reaching from his tactical forces back to information assets in the United States.[18] Clausewitz's advice that lines of communication "must not be permanently cut, nor must they be too long or difficult to use"[19] is fair warning to the operational commander that he must understand how his LOCs function and how well they are protected.

The failure to provide adequate strategic protection to IT assets is real.[20] The July 15, 1996 Executive Order establishing the President's Commission on Critical Infrastructure Protection is a step in the right direction. Critical assets include telecommunications, electrical power systems, gas and oil storage and transportation, and banking and finance. The executive order identified both physical threats and "cyber threats" against which the commission was tasked to develop a strategy of defense ensuring that the government and private sectors work together because of the extensive integration of systems and interests.[21]

The efforts of the commission are outside of the operational commander's direct purview. Nonetheless, understanding that the risk to his IT LOCs extends back to the homefront, he will be better able to judge the robustness of the information architecture on which he relies and develop his own plan for operational protection.

At the operational level two factors drive the requirement for operational protection of IT assets, their value and the threat environment. A third factor, the capability to provide an effective defense, will influence the commander's approach depending upon the specific asset/threat combination.

Value of IT and IW assets

IT brings tremendous value to the operational commander's table. Its ability to synthesize intelligence and surveillance data into a fused picture enhances the commander's ability to achieve solid awareness of the activity within the battlespace and to ascertain the strengths and weaknesses of his adversary. The ability to communicate graphically and verbally with levels

above, below, and across, helps maintain synchronization and control, and minimizes confusion. IW-O assets such as sensors and weapons guidance systems provide indications and warnings of attack and allow precision strike. Of particular importance to the commander are his C2 Support (C2S) Systems.

The commander relies extensively upon his C2S systems to enable him to accomplish the functions of C2. C2S systems must reliably provide information that is relevant, essential, timely and in quickly understandable and usable form. An electronic extension of the commander's thought process, they allow him to stay ahead of his adversary in the decision cycle. They are his principle tool to collect, transport, process and disseminate information.[22] Essential to success, they are the IT assets most keenly targeted by C2W, the "anti-head, anti-neck" attack and the most developed form of IW-O. Targeted at breaking down the military leader's decision capability, C2W yields the highest IW-O pay-off.[23]

What happens when these systems are degraded? A study conducted at the Naval Postgraduate School in 1994 demonstrated how degradation of information flow directly affects mission accomplishment. By slowing information transfers about adversary movements or about partner movements, both mission accomplishment and rate of mission accomplishment were reduced. The impact was especially clear for operations crossing boundaries between operational areas. Slowing both information transfers did not yield a sum of their individual effects – the impact was was magnified.[24] The simulated effect was a slow-down of the decision cycle and increasing uncertainty. The same effect taking place in reality is unacceptable.

Threats to IT Assets

Clausewitz cautions the commander who forays deep into enemy territory that he will have "very long and vulnerable lines of communication, whose chief weakness, however [sic], lies in their being always and everywhere exposed to attacks by an insurgent population."[25] This is especially true for the extended LOCs supporting the operational commander's theater IT assets. The insurgent attack can be waged in or out of theater, and the attacker need not be physically present. The operational commander cannot assume that because his opponent is technologically backwards he will not be capable of executing an effective attack against IW and IT assets. Attacks can be launched with inexpensive, commercially available equipment and the talent to use the equipment can be hired or trained at similarly low costs.

IT and IW assets are also exposed to risk due to natural disasters such as floods or lightning storm. The human factor has great impact on the security of the commander's systems. It can wreak havoc through simple error, inadequate doctrinal training (*i.e.*, the misuse of the IT or IW tool), laziness (leading to lax attitudes about security), or even deliberate sabotage actions. These factors add up to a situation in which it is impossible to eliminate all risk that accompanies dependence upon IT and IW assets.

A Strategy for Risk Management

> **Because 100 percent protection of information is not possible all of the time, risk management rather than risk avoidance is necessary.[26]**

Operational Risk Management (ORM) adopts a risk versus benefit philosophy to help the operational commander apply the best level of controls to

a mission or operation. The objective is to undertake risk with a solid understanding of what one faces, knowing that risks have been identified, assessed and controlled where possible. It has been used successfully to minimize risk across a broad range of activities. "Military units have reduced their mishap rate up to 60 percent by using operational risk management (ORM)."[27] Naval Warfare Publication 1 states, "Risk Management is a formal, essential tool of operational planning. Sound decision making requires the use of this tool both in battle and in training."[28] It is based on four basic principles[29]:

- Know the risk
- Accept no unnecessary risk
- Make risk decisions at the appropriate level to establish clear accountability
- Accept risk when benefits outweigh the costs

The basic process is simple. Consider the mission in question. Identify any hazards associated with each step of the mission. Develop means to control or eliminate each hazard for each step. Identify alternate means to do the step in the event it fails despite efforts to control its risk. Compare the risks of each step to the value-added it contributes to the mission. Make control decisions based on cost-benefit comparison. Review control actions then rehearse the plan.

This careful review of the planned mission and alternate steps essentially pre-programs personnel to recognize when things are starting to go awry. Observations will translate into recognition and orientation more quickly. Decisions will already have been thought through. And actions can be taken almost immediately. In a nutshell, ORM sides with Murphy. What can go wrong, will go wrong. One had better be ready for it.

Applying ORM to IT/IW Operational Protection

Developing a scheme of operational protection for systems is not the same as planning a mission. Nonetheless, the dependence on these assets makes them stand out as mission vulnerabilities. ORM principles apply.

Risk Assessment

The first step in applying ORM to IT/IW operational protection is the most difficult because of the wide range of risks involved both in and out of theater. Effective hazard identification is the key to success. Once each hazard is identified, controlling mechanisms can be put in place. If a control isn't possible, at least the potential for being surprised will be reduced as the process provides an education to recognize attacks (or system failures) in the making.

"Successful protection of the Army battle command system starts with an understanding of how others will seek to degrade or exploit it."[30] Friendly forces must evaluate themselves from the enemy's eyes to determine the best estimate of what the enemy views as their critical assets. Advice for planning an IW attack is to evaluate systems, networks and facilities as to their usefulness as targets; give them a level-of-effort; and allocate resources to take them.[31] By shifting perspective, a sound defensive approach is realized. Evaluate own systems as to their usefulness to the enemy as targets, estimate how much effort he would be willing to make against them and allocate resources to defend them.

Joint effort of intelligence and IW personnel is critical to success in this phase. An effective information assurance strategy calls for identification of critical nodes and links and an assessment of an adversary's capabilities and

intentions.[32] Intelligence will be needed on potential forms of attack including technical parameters, operating procedures, employment doctrine and vulnerabilities of adversary C2-attack equipment and weapons systems. The style and capability of the adversary's reconnaissance, surveillance and target acquisition process, their evaluation of critical friendly command and control nodes and high-value targets, adversary doctrine and capabilities for the use of psychological operations and military deception all must be investigated."[33] Complicating the intelligence problem is the fact that much of this activity will need to be done during routine peacetime. The "adversary" won't be known. This information will be needed for a variety of adversary profiles and for specific adversaries identified as "likely suspects."

In addition to the risk of enemy attack within theater, the ORM process must also assess the risk to strategic IT assets. The operational commander will not be able to directly control actions taken to defend those assets, but he is in a position to minimize his risk by pressing for high readiness in theater as soon as possible. For example, "Logistics information systems tend to be both elaborate and critical to successful military operations and yet generally subject to less stringent security measures than other military information systems."[34] The force will be most threatened by the vulnerability of logistics systems during mobilization and movement into the theater of operations. Once in theater the commander can demand quick action on the part of his forces to ensure supply requirements are reviewed and acted on daily. He can press for a local database to track personnel and supplies once they have entered the theater. In the event

logistics databases in the U.S. are attacked, he can isolate his local database and use it to maintain accountability of the logistics assets within his control.

His extended LOCs are another vulnerability that he does not control, but must consider in his plans. Alternate channels must be identified and tested. Communications and circuit shifts between options must be drilled. Peacetime "breakdowns" in the extra-theater LOCs should be noted, reported and followed until they are resolved. The problem is so large that no one wants to take responsibility. The operational commander must force the issue.

Consideration of alternate channels should not be bounded by established options. "Lines of communication will, of course, have been set up at home, but the army is not necessarily tied to them; if need be, it can leave them and use any road available."[35] This is as true today as it was in Clausewitz's time. A willingness to leave the beaten path builds in a kind of serendipitous redundancy. Consider that in 1944, during the Battle of Arnhem the British First Airborne Division landed with the wrong radio crystals and believed their communications were were cut off. Throughout the battle the national telephone system was fully functional. Had the paratroopers thought "outside the box" for alternate solutions, or had they identified this alternative prior to the operation, they could have easily found access to a link with their command element.[36]

Use of IT brings on other common risks. Some of these and potential controls for them are:

Information Overload – Information flowing from echelons above and below threaten to swamp the operational commander and reduce his battlespace

awareness. The operational commander must take advantage of systems designed to help filter this information and format it intelligibly. He must be familiar with how they work to ensure they reflect his approach to data filtering and so he can trust them. This applies equally to systems managing data such as message handling and dissemination systems and "fused picture" battlespace displays. The commander must understand their capabilities and limitations and ensure his people know how to use them. Alternates to such systems are staff members who can be trusted to provide a similar filtering mechanism in the event of system failure.

System Overload – Required information volumes expected for full spectrum intelligence analysis in future conflicts is beyond the capacity of current systems. The increase of several orders of magnitude may overwhelm our ability to collect, analyze, store and disseminate results.[37] As William James said, "The art of being wise is the art of knowing what to overlook."[38] Recognition of this must drive intelligence collection and analysis to yield information "that can be suitably digested and acted upon."[39] It will also protect the intelligence staff from becoming overwhelmed.

Communications demands can also overload system capacity, especially in networked systems. Localized degradations of response time and brownouts of internet service due to fluxes in demand have occurred in the commercial sector. The expected surge in communications requirements that accompanies crisis action could yield similar problems for theater networks. Stress testing programs are available which allow simulations of live loads to identify potential

transmission bottlenecks before a real crisis takes place.[40] Corrective action in the form of system upgrades or in procedural restrictions to prevent system overload can then be put in place as necessary.

Hardware Failure – Normal wear and tear causes systems to fail. The harsh environment of deployed settings and the act of movement to the theater increases the risk to hardware. Hot spares and well-trained technicians are the best control for the risk that your hardware may suddenly cease working. Strict maintenance and test cycles also minimize risk of unexpected failure.

Interoperability Problems – The commander cannot anticipate "plug and play" system operations. Much of the initial set-up time for theater IT will be devoted to wringing out problems caused by differing protocols and system configurations of the services. This is not just a joint issue. Elements shifting from one theater to another and reconnecting to same service systems must readjust protocols and procedures because of stovepiped development and application.[41] Efforts to solve this problem include the establishment of a single, unifying DoD joint technical architecture intended to drive all future DoD C4ISR acquisitions.[42] This will help in the future. Today the operational commander must place high priority on securing technical training for his systems administrators and maintainers at schools of the various services to minimize set-up time and anticipate that it will not be fast or easy.

Doctrine Problems – "In many cases, the technology associated with a new system or piece of equipment is mature and the technical risk low, but we do not know how to effectively use it, and so the operational risk is high."[43] When

advanced technology is fielded without ample time to learn how it is operated and how it is employed, the operational commander invites mistakes. He must fight the temptation to accept every "new toy" that comes along. Use of technology coordination (or cut-off) dates (TCDs) to prevent late insertion of technology to satisfy someone else's agenda can help ensure forces train as they will fight.

A fruitful way to verify that as many system vulnerabilities as possible have been uncovered is to form "red teams," aggressors to attack systems during planned tests, exercise and demonstrations. Their efforts to find vulnerabilities and ways to exploit them gives a dual pay-off. First, they enable the development of ways to defend against similar attacks from the real enemy and second, they may identify new ways to attack the enemy.[44]

Eliminate Unnecessary Risk

Eliminating unnecessary risk is the next step of the ORM process. A good hard look at procedures and systems can eliminate risk without any real pain in terms of effort, resources or expected outcomes. There are many "easy outs" in the IT world. Examples include installation of uninterruptable power sources (UPSs) and back-up generators, ensuring personnel are disciplined about performing back-ups and keeping passwords current and allowing adequate time for system maintenance. Additional risk can be eliminated (or greatly reduced) by insisting on redundant or compatible systems whenever possible.

Create enclaves of security by isolating systems that do not absolutely need to be tied to external systems to support theater operations. These "trusted" systems can be scaled from individual computers to larger networks.

Because they are not connected to the outside world, outsiders cannot penetrate them. Of course, all data and software must be thoroughly validated as "virus free" before it enters the enclave. Development and installation of trusted firewalls may allow a connected enclave, *i.e.*, one that is shielded from the outside, but has protected connections to other trusted enclaves or limited connections to less restrictive networks.[45]

Make Risk Decisions

Once unnecessary risk has been eliminated, it is time for the tougher decision. What risk is inherent in the mission? Can any mission elements be sacrificed for risk reduction? The key to these decisions is that they must be made at an appropriate level of command. If the operational commander delegates this decision-making he should, at a minimum, insist upon a thorough brief on the chosen approach to acceptable and unacceptable risks.

Accept Risk Based on Benefits and Costs

The risk decisions themselves will be driven by the cost of eliminating or decreasing the risk in terms of resources, personnel efforts, or interference with function and/or mission. If certain data is more important, or a system's function is critical, more costs are justified. Nonetheless, costs may be prohibitive if rapid access and reach-back is integral to operations.

Planning for Success -- Rational Expectations

Organize for Success

Defensive IW (IW-D) must be planned as a system. To accomplish this most effectively, a rational organization combining systems expertise and

operational acumen is required.[46] "Integrated technologies demand more integrated organizational support structures...In a joint environment, the JFC must mandate a unified communications/information systems team."[47] This team of experts can effectively implement the ORM process with proper mission focus complemented by a real understanding of systems integration and vulnerability issues. It may be focused on IW-D alone or both IW-D and IW-O. Most effectively implemented as a permanent element, it should be led by the J6 organization and include additional duty members from the J2 and J3 staffs.

Additional ORM Benefits

The education of the ORM process provides additional means to reduce risk. Increased understanding of how system attacks may be launched allows the design of an effective indications and warning (I&W) profile. This profile can help establish threshold criteria for intelligence collection and automated detection agents to provide alerts as early in an attack as possible.[48] Such a "trip wire" strategy is critical given how quickly damage to IT assets can take place.[49]

Develop a Scheme for System Defense

A final product of the ORM process must be the operational commander's scheme for system defense. A reasonable scheme builds on Alberts' "defense-in-depth" strategy. Its variable information availability depending upon severity of threat fits well with the ORM approach. This scheme shifts system access from "information first" to "security first" with increasing levels of access controls, sophistication of defense and cost.[50] Crossing each barrier requires an IW attack of increasing sophistication and cost.

No scheme of defense is complete without a plan to conduct damage control. The IW and Operations staffs must assume that an attack will occur and will cause some damage. With this in mind, they must prioritize systems and circuits for reconstitution. Fall backs using the assets of lesser important systems and focused repair efforts must be automatic.

The final scheme must be based on readiness, prevention of intrusions, user education and discipline, planned alternates, constant efforts to detect "insurgencies," a comprehensive damage control plan, and tightened access controls upon indications that attack may be imminent. Clausewitz sums it up,

> **One can mitigate the situation somewhat by taking some fortresses near the army's position and on the roads that lead back from it, or, where there are no fortresses, by fortifying appropriate points; by treating the population well, keeping strict discipline on military roads, policing the area thoroughly, and constantly keeping the roads in repair. But the risks can never be entirely eliminated.**[51]

Conclusions

In the IW arena an adversary can strike hard with but a small offense. Dependence on technology makes one highly vulnerable to attack. The only rational answer is to invest in a credible defense to reestablish equilibrium between the offense and defense.[52] To do so takes time, money and personnel. Operational commanders must exhaust their own options to minimize risk and exposure. It is impossible to eliminate all risk, but risk can be driven down to an acceptable level. By following a structured methodology such as that outlined in this paper, the operational commander increases the likelihood that he will secure his lines and win the information war.

Notes

[1] *Information Warfare: A Strategy for Peace...The Decisive Edge in War*, Chairman's Comments.

[2] Information networks are the focus of concern. *A National Security Strategy of Engagement and Enlargement, 13, 25.*

[3] *National Military Strategy of the United States of America*, 15.

[4] Stephen Kent, chief scientist for security technology, Bolt Beranek and Newman, Inc., as quoted by Anthes in "Security Pundits Weigh War Threats."

[5] Rowe, 2.

[6] Joint Pub 3-13.1, I-3.

[7] This is similar to conventional weapons providing protection for support functions such as medical or logistics services. The protected assets are not considered weapons or part of the weapons employment doctrine, but they are sufficiently important to merit the dedication of forces to their protection.

[8] Alberts, 3.

[9] Of course, this is assuming that the location of the stand-alone and the fact of its existence are covered by operational security practices to minimize risk of physical attack.

[10] "Crucial Network Imperatives Spawn Information War Peril," 35.

[11] "Battlespace Information: Command and Control (C2), Operational Intelligence and Systems Integration," 22.

[12] "Crucial Network Imperatives Spawn Information War Peril," 35.

[13] *Joint Pub 3-13.1*, I-3.

[14] "Report of the Defense Science Board Task Force On Information Warfare – Defense (IW-D)"

[15] Schwartau, 13.

[16] "Operational Functions," 32.

[17] Ibid.

[18] LOCs are typically viewed as logistical lines allowing movement and sustainment of forces. When considering IT assets and information flow these lines can be taken literally. They provide the communications link from the national-strategic level through the operational and tactical levels and between similar levels of supporting and supported commands. As the integrity and strategic protection of logistics LOCs is critical to sustaining the forces, the integrity and strategic protection of information LOCs is critical to sustaining information flow.

[19] Clausewitz, 345.

[20] Many sources back up Schwartau's claim that the U.S. continues to be vulnerable to enemy attack on our systems, especially those within our borders. "That Wild, Wild Cyberspace Frontier,"

"Western Infrastructures Face Rogue Data Stream Onslaught," "Crucial Network Imperatives Spawn Information War Peril," and "No Sheriffs Patrol Universal Cyberspace Frontier Towns" are representative of the increasing level of attention the NII vulnerability is receiving. Although published in 1994, Schwartau's seminal publication, *Information Warfare: Chaos on the Electronic Superhighway* is an extremely comprehensive and frightening discourse on the growing threat.

[21] *Executive Order on Critical Infrastructure Protection.*

[22] *Joint Pub 6-0*, I-3.

[23] Libicki, What is Information Warfare? 9-18.

[24] Dishong's detailed analysis is not an adequate measure for definitive conclusions. Nonetheless, it does provide solid support for intuitive assessments and validates an approach to modeling the impact of IT on the commander.

[25] Clausewitz, 347.

[26] "Redundancy, Robustness Protect Vital National Information Links," 38-9.

[27] U.S. Navy Safety Center Website, <http://www.norfolk.navy.mil/safecen/orm.htm>

[28] OPNAVINST 3500.39.

[29] "Operational Risk Management: A Moral Imperative."

[30] Blount, 14.

[31] Eisen, 6.

[32] "Redundancy, Robustness Protect Vital National Information Links," 38-9.

[33] Blount, 14.

[34] Kraus, 44.

[35] Clausewitz, 345.

[36] *Joint Pub 3-13.1*, I-2.

[37] Until recently a volume of approximately a gigabyte (10^9 bytes) of data was needed to support one day's operational intelligence in a typical theater-level intelligence center. Today's requirements are in the multiple terabyte (10^{12} bytes) range. See Black, *This Page Under Construction: Information Warfare in the Post-Cold War World*, 17.

[38] Correct Quotes, Version 1.0.

[39] Kaminsky, "21st Century Battlefield Dominance," 2.

[40] "Overloads Strike Networks; Brownouts, Failures Loom," 23.

[41] "Redundancy, Robustness Protect Vital National Information Links," 37.

[42] Paige, 2.

[43] Kaminski, "Creating Opportunity with Advanced Technology," 1.

[44] Robinson, "Army Information Operations Protect Command and Control," 47-8.

[45] Anderson and Hundley, 42-43.

[46] Several authors have proposed an additional branch of the military devoted specifically to IW, an Information Corps. Libicki discusses this concept fully in *The Mesh and the Net,* 52-69.

[47] "Battlespace Information: Command and Control (C2), Operational Intelligence and Systems Integration," 23.

[48] The Joint Command and Control Warfare Center (JC2WC) and the Information Warfare centers of each service can provide excellent guidance on "sniffers" and "snoopers" to identify any "rogue" activity on networked systems. These commands are also excellent sources of specialized talent for systems engineering, operations, and technical analysis of capabilities and vulnerabilities.

[49] Robinson, "Information Warfare Strings Trip Wire Warning Strategy," 29.

[50] Alberts, 39-41.

[51] Clausewitz, 347.

[52] Arquilla and Rondfeldt, 93.

Bibliography

Alberts, David S. *Defensive Information Warfare*, Washington: Center for Advanced Concepts, Technologies, and Information Strategies. August, 1996.

Anderson, Robert H. and Richard O. Hundley. *Security in Cyberspace: An Emerging Challenge for Society*. Santa Monica: RAND. 1994.

Anthes, Gary H. "Security Pundits Weigh War Threats." *Computerworld*. October 2, 1995. <http://www.computerworld.com/search /data/cs_950101-951002SL38secure.html> (28 April 97).

Arquilla, John and David Ronfeldt. *The Advent of Netwar*. Santa Monica: RAND. 1996.

Black, LTC Steven K. *This Page Under Construction: Information Warfare in the Post-Cold War World*. Ridgway Viewpoints No. 96-1. Pittsburgh: Matthew B. Ridgway Center for International Security Studies.

Chief of Naval Operations. "OPNAV INSTRUCTION 3500.39 Operational Risk Management." <http://www.norfolk.navy.mil/safecen/ormfin.doc> (May 5, 1997).

Clausewitz, Carl von. *On War*. edited by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1996.

Blount, Kerry A. "Wrestling with Information Warfare's 'Dark Side'." *Army*, February 1996.

Clausewitz, Carl von. *On War*. edited by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1996.

Correct Quotes Version 1.0. Novato, CA: Wordstar International Inc. 1972.

"Crucial Network Imperatives Spawn Information War Peril." *Signal*. June 1996.

Dishong, Donald J. "On Studying the Effect of Information Warfare on C2 Decision Making" Naval Postgraduate School, Monterey, CA, June 1994.

Eisen, LTC Stefan, Jr. "Netwar, It's Not Just for Hackers Anymore." Unpublished Paper. Newport: U.S. Naval war College, 22 June 1995.

"Executive Order on Critical Infrastructure Protection." Washington: The White House. July 15, 1996.

Johnson, LTC(P) Robert E. "Information Warfare: Impacts on Command and Control Decision-Making." Carlisle Barracks, PA: U.S. Army War College. 1996.

Joint Chiefs of Staff. *Information Warfare: A Strategy for Peace...The Decisive Edge in War.* Washington: Department of Defense. 16 June 1995.

_____ *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations, Joint Pub 6-0.* Washington: Department of Defense. 30 May 1995.

_____ *Joint Doctrine for Command and Control Warfare (C2W). Joint Pub 3-13.1.* Washington: Department of Defense. 7 February 1996.

_____ *National Military Strategy of the United States of America: A Strategy of Flexible and Selective Engagement.* Washington: Department of Defense. February 1995.

Joint Military Operations Department. "Operational Functions." Newport: U.S. Naval War College, August 1996.

_____ "Battlespace Information: Command and Control (C2), Operational Intelligence and Systems Integration." Newport: U.S. Naval War College, November 1996.

Kaminski, Paul G. "21st Century Battlefield Dominance" Prepared remarks delivered to the American Defense Preparedness Association and Association of the U.S. Army Symposium, Redstone Arsenal, AL, January 16, 1996.

Kaminski, Paul G. "Creating Opportunity with Advanced Technology" Prepared remarks delivered to the Advanced Concept Technology Demonstrations Manager's Conference, Defense Systems Management College, Fort Belvoir, VA, September 10, 1996.

Kraus, CDR George F., Jr., U.S. Navy (Retired). "Information Warfare in 2015." *Proceedings.* August 1995.

Libicki, Martin C. The Mesh and The Net. Washington: Institute for National Strategic Studies, National Defense University. 1994.

_____ What is Information Warfare? Washington: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University. August 1995.

National Command Authority. *A National Security Strategy of Engagement and Enlargement.* Washington: The White House. February, 1996.

"No Sheriffs Patrol Universal Cyberspace Frontier Towns." *Signal.* June 1996.

"Operational Risk Management: A Moral Imperative." Air Education and Training Command (AETC) Operational Risk Management (ORM) Website, <http://www.aetc.af.mil/se2/orm.htm> (May 5, 1997).

"Overloads Strike Networks; Brownouts, Failures Loom." *Signal.* July 1996.

Paige, Emmet Jr. "Ensuring Joint Force Superiority in the Information Age." Prepared remarks delivered to the Armed Forces Staff College, Norfolk, VA, July 30, 1996.

"*Redundancy, Robustness Protect Vital National Information Links.*" *Signal.* May 1996.

"Report of the Defense Science Board Task Force On Information Warfare – Defense (IW-D)." Washington: Office of the Under Secretary of Defense For Acquisition and Technology. November 1996. <http://jya.com/iwd.htm#6.0> (March 17, 1997).

Robinson, Clarence A., Jr. "Information Warfare Strings Trip Wire Warning Strategy." *Signal.* May 1996.

Robinson, Clarence A., Jr. "Army Information Operations Protect Command and Control." *Signal. July* 1996.

Rowe, Wayne J. "Information Warfare: A Primer for Navy Personnel." Strategic Research Department Research Report 6-95, Newport: U.S. Naval War College. 23 June 1995.

Schwartau, Winn, *Information Warfare: Chaos on the Electronic Superhighway.* New York: Thunder's Mouth Press, 1994.

"*That Wild, Wild Cyberspace Frontier.*" *Rand Research Review.* Fall 1995. <http://www.rand.org/publications/RRR/RRR.fall95.cyber/wild.html>.

U.S. Navy Safety Center Website. <http://www.norfolk.navy.mil/safecen /orm.htm> (May 5, 1997).

"*Western Infrastructures Face Rogue Data Stream Onslaught.*" Signal. January 1996.